Attachment B

Geofencing

As part of the January 2019 Task Force meeting, VT-ARC presented on the concept of carrier-based geofencing as a potential CIS solution, and CTIA identified some legal and privacy issues associated with the concept of geofencing as a CIS solution. Below is a summary.

In the contraband phone context, geofencing would mean that a carrier determines whether a mobile device is located within the geographic boundary of a correctional facility and restricts or disables cellular services if the device is not authorized to operate in that area. Today, carrier-based geofencing is a theoretical concept and is not deployed as a current CIS solution. As described below, existing wireless network architectures and device monitoring capabilities present a number of technical challenges and legal and privacy issues surrounding such a solution.

VT-ARC Overview of Geofencing Approaches. Current cellular standards allow two types of geolocation: fine location, in which, during (for example) a 9-1-1 call, the device sends a GPS-based location measurement to the network; and coarse location, in which a carrier determines location by assessment of cell signals from nearby cell towers.

GPS-based fine location principally relies on satellite connectivity and can often identify a device's location to within 10 meters, but it is not reliable in the correctional facility environment. First, buildings in these facilities are typically constructed of concrete and steel, which block the satellite signals that GPS uses. In addition, hacked phones can spoof their GPS locations and send false data to the network. By contrast, the MAS solutions in the Testbed (and similarly designed solutions) do not depend on GPS to determine whether or not a phone is located in a correctional facility.

Although coarse location suffers less from these drawbacks, it is not sufficiently precise and creates challenges for geofencing. Based on calculations performed using typical cell tower densities, facilities in rural areas are often near only one or two cell towers, resulting in device signal assessment that cannot reliably identify location within an area of 10 km; granularized assessment (*i.e.,* triangulation) requires three towers to locate a device with a precision of 50 meters. In urban environments, towers may be sufficiently dense to allow three-tower triangulation around correctional facilities, but 50 meter precision often is not sufficient to positively determine whether or not a device is within a facility's geographic boundary. As a result, geofencing in both rural and urban environments poses a substantial risk of sweeping in lawful wireless users outside of correctional facilities.

Furthermore, the location services supported by carriers' networks are not designed to sweep or scan a given area to precisely locate and identify all devices within that area, contraband and non-contraband alike, as geofencing would require. Instead, carriers' current location services are designed to locate a specific device when prompted. For example, when a customer dials 9-1-1, his or her phone automatically triggers a location query by the carrier. Similarly, and in accordance with existing privacy regulations, location services also may be triggered when the user has expressly opted in to sharing that information. Modifying cellular networks to constantly track and identify every cellular device in the vicinity of a correctional facility would require new network capabilities that are not part of existing deployment plans.

CTIA's Review of Legal and Privacy Issues Surrounding Geofencing. Chairman Pai directed the Task Force to work together "to stop the threat of contraband cellphones without causing harm to legitimate wireless users." To that end, CTIA undertook a review of geofencing in the context of Federal privacy and consumer protection laws that limit how wireless carriers may collect, use, and disclose location information. In CTIA's view, these laws raise difficult legal issues in the context of the use of proposed geofencing approaches to contraband issues, because geofencing would require tracking of – and potential disruption (albeit inadvertent) of service to – many legitimate users of wireless services. MAS solutions avoid many or all of these issues because their coverage is limited to the interior of correctional facility perimeters.

Section 222 of the Communications Act protects customer proprietary network information, including location information, of mobile voice customers, generally restricting the use and disclosure of such information.[1] These restrictions are subject to narrow exceptions, and there is no precedent for exempting the use or disclosure of location information to determine whether a device should be blocked or disabled as contraband.

In addition, the Commission has interpreted Section 201(b) of the Communications Act to generally prohibit carriers from blocking calls, except in limited circumstances that are not relevant to geofencing.[2] Blocking calls from legitimate users' devices raises additional issues that would need to be resolved.

---

[1] *See generally* 47 U.S.C § 222.

[2] *See, e.g., Establishing Just and Reasonable Rates for Local Exchange Carriers*, Declaratory Ruling and Order, 22 FCC Rcd 11629, ¶¶ 1, 6 (WCB 2007) (clarifying that carriers cannot block, choke, reduce, or restrict traffic in any way); *see also Connect America Fund*, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663, ¶ 974 (2011) (prohibiting interconnected and one-way VoIP services from blocking voice traffic to or from the Public Switched Telephone Network).

Finally, where non-common carrier services are concerned, Section 5 of the FTC Act protects consumers from unfair or deceptive acts or practices.[3] The fact that geofencing may involve *en masse* location tracking of all phones in the vicinity of a correctional facility – including lawful users who may receive no notice of geofencing and have no ability to avoid the practice – over long periods of time could expose wireless providers to FTC investigation and possible enforcement actions.

Geofencing Summary. Although under current law carrier-based geofencing is likely infeasible in the U.S. for the legal and technical reasons described above, other technological approaches could provide similar geolocation capabilities that MAS and other vendors and correctional facilities would implement and administer. Such approaches require further discussion and development, and CTIA and its members intend to coordinate with MAS vendors, the correctional community, and other stakeholders to explore them more thoroughly.

[3] *See* 15 U.S.C. § 45(a)(1).

Attachment C

Contraband Phone Task Force Member Organizations

1. Alabama Department of Corrections
2. Arkansas Department of Correction
3. California Department of Corrections and Rehabilitation
4. Indiana Department of Correction
5. Mississippi Department of Corrections
6. Oklahoma Department of Corrections
7. South Carolina Department of Corrections
8. Tennessee Department of Correction
9. Texas Department of Criminal Justice
10. Association of State Correctional Administrators
11. U.S. Department of Justice, Bureau of Prisons
12. CTIA
13. AT&T
14. Sprint
15. T-Mobile
16. Verizon

ASSOCIATION OF STATE CORRECTIONAL ADMINISTRATORS

Executive Committee
President, John Wetzel
Vice President, Colette Peters
Treasurer, Anne Precythe
Past President, Leann Bertsch

Regional Representatives
Northeast, Marcus Hicks
Southern, Jefferson Dunn
Midwest, Heidi Washington
Western, Chuck Ryan

The Members of the Association of State Correctional Administrators (ASCA) are the leaders of each U.S. State corrections agency, Los Angeles County, the District of Columbia, New York City, Philadelphia, the Federal Bureau of Prisons, US Military Correctional Services (Army, Navy, Air Force, Marines), and any United States territory, possession, and/or commonwealth. Each member is an executive level appointee and works hand in hand with their administration to implement and set correctional policy for their state or region.

Our members, primarily cabinet-level officials, oversee 400,000 correctional professionals and approximately 8 million inmates, probationers, and parolees.

For more than a decade contraband cell phones have infiltrated correctional facilities across our nation and around the globe. Kidnapping, extortion, bribery, witness intimidation, robbery, identity theft, malware attacks, security breaches, and other serious crimes are being orchestrated on these smuggled devices. Illegal cell phones are making their way behind prison walls in large numbers through various means, including by drones, through corrupt staff and vendors, and even in body cavities.

ASCA Headquarters * P.O. Box 102 * Iona, Idaho 83427
Phone * (208) 557-8264 WWW.ASCA.NET

ASSOCIATION OF STATE CORRECTIONAL ADMINISTRATORS

Executive Committee
President, John Wetzel
Vice President, Colette Peters
Treasurer, Anne Precythe
Past President, Leann Bertsch

Regional Representatives
Northeast, Marcus Hicks
Southern, Jefferson Dunn
Midwest, Heidi Washington
Western, Chuck Ryan

The partnership between CTIA and ASCA has been productive and appreciated. We have learned a great deal from our meetings, and we respect the work and challenges that we each face. Although we continue to work together to fight contraband cellphones in prisons, state and local correctional institutions need access to the full complement of tools. Tools that include Managed Access Systems, Micro-jamming, geo-fencing, and all other technologies must be on the table to help solve this problem.

We are asking for more in-depth testing for tools such as micro-jamming, and assistance in making all options legal to use within correctional facilities.

Sincerely,

Jefferson S. Dunn, Col(r), USAF
Commissioner
Alabama Department of Corrections
Executive Committee Member
Association of State Correctional Administrators (ASCA)